AMENDMENTS

In the Claims:

1. (Previously Presented) A computer system, comprising:

memory; and

a security application configured display a list of security rules to a user and to enable ones of said security rules based on user inputs, said security application configured to lock down resources of said computer system by modifying security settings of said computer system based on which of said security rules are enabled when an activation request is received by said computer system, said security application configured to store, in said memory, data indicative of said security settings, said security application configured to perform comparisons between said data and said security settings and to determine when one of said security settings has changed from a first value to another value based on one of said comparisons, said security application further configured to change said one security setting to said first value in response to said one comparison.

2. (Original) The system of claim 1, wherein said security application is further configured to transmit a message indicating that said one security setting has changed in response to said one comparison.

3. (Original) The system of claim 1, wherein said security application is further configured to store said data in response to said activation request.

4. (Original) The system of claim 1, wherein said security application is further configured to periodically compare each of said security settings to said data.

5. (Original) A system for locking down resources of computer systems, comprising:

means for receiving a request for activating a security profile;

means for modifying security settings of a computer system in response to said request;

means for storing data indicative of said modified security settings;

means for automatically determining when one of said security settings has changed from a first value to another value by periodically comparing said data to said security settings; and

means for automatically changing said one security setting to said first value in response to a determination by said determining means that said one security setting has changed.

6. (Original) The system of claim 5, wherein said system further comprises:

means for automatically transmitting, in response to said determination, a message indicating that said one setting has changed.

7. (Original) The system of claim 5, wherein said storing means is configured to store said data in response to said request.

8. (Previously Presented) A method for locking down resources of computer systems, comprising:

receiving a request for activating a security profile;

modifying security settings of a computer system in response to said request;

storing data indicative of said security settings, as modified by said modifying;

automatically determining when one of said security settings has changed from a first value to another value by periodically comparing said data to said security settings; and

automatically changing said one security setting to said first value in response to a determination in said determining that said one security setting has changed.

9. (Previously Presented) The method of claim 8, further comprising:

automatically transmitting, in response to said determination, a message indicating that said one security setting has changed.

10. (Previously Presented) The method of claim 8, wherein said storing is performed in response to said request.

11. (Previously Presented) The system of claim 1, wherein said security application is configured to change said one security setting in response to said one comparison without changing another of said security settings in response to said one comparison.

12. (Previously Presented) The system of claim 1, further comprising an operating system configured to analyze said one security setting to determine whether access to a resource of said computer system is restricted.

13. (Previously Presented) The computer system of claim 12, wherein said one security setting is associated with one of said security rules, and wherein said operating system is configured to enforce said one security rule based on said one security setting.

14. (Previously Presented) The computer system of claim 13, wherein said security application is not configured to enforce said one security rule.

15. (Previously Presented) The computer system of claim 12, wherein said security settings are within a machine state analyzed by said operating system for selectively enforcing said security rules.

16. (Previously Presented) The computer system of claim 15, wherein said data is separate from said machine state and is stored in said memory by said security application in response to said activation request.

17. (Previously Presented) The computer system of claim 16, wherein said one security setting is a flag associated with said resource.

18. (Previously Presented) The system of claim 5, further comprising an operating system configured to analyze said one security setting to determine whether access to a resource of a computer system is restricted.

19. (Previously Presented) The method of claim 8, wherein said one security setting is analyzed by an operating system of said computer system in order to control access to a resource of said computer system.

20. (Previously Presented) A computer system, comprising:

memory;

an operating system configured to analyze a machine state to control operation of said computer system, said machine state including a security setting associated with a resource of said computer system and indicating whether access to said resource is restricted, wherein said operating system is configured to analyze said security setting to control access to said resource; and

a security application configured to modify said security setting based on a user input and to store, in said memory, data indicative of a state of said security setting, as modified by said security application, said security application configured to perform a comparison between said data and said security setting to detect an unauthorized change of said security setting, said security application further configured to automatically change said security setting based on said data in response to a detection of an unauthorized change of said security setting.

21. (Previously Presented) The computer system of claim 20, wherein said security application is configured to set said security setting based on said user input in response to a user activation request.

22. (Previously Presented) The computer system of claim 21, wherein said security application is configured to store said data in said memory in response to said user activation request.

23. (Previously Presented) The computer system of claim 20, wherein said security setting is a flag stored within a register.

24. (Previously Presented) The computer system of claim 20, wherein said security application is further configured to transmit, in response to said detection, a message indicating that said one security setting has changed.